FGV EBAPE

RAP
BRAZILIAN JOURNAL OF PUBLIC ADMINISTRATION

Article

External oversight of Intelligence activities in the digital age: An exploratory model

Conrado Klöckner [1]

Luiz Antonio Joia [1]

[1] Fundação Getulio Vargas / Escola Brasileira de Administração Pública e de Empresas, Rio de Janeiro - RJ, Brazil

This study develops an exploratory model to assess the external oversight of a country's intelligence activities based on a narrative literature review. This process revealed key elements that characterize a high-quality accountability system, which were mapped and structured into an analytical model. Additionally, it led to a clear definition of the construct "oversight capacity" and offered an overview of the current literature on external oversight of intelligence activities. The proposed model serves as a valuable tool for case studies and comparative analyses, thereby facilitating the diagnosis of weaknesses in the accountability system and supporting discussions that may contribute to refining the model itself. Its use can improve methodological consistency in this area of study, leading to a more comprehensive understanding of the subject, promoting comparisons of results, and helping to generate hypotheses for future tests. Regarding its limitations, (i) the model is exploratory and, therefore, remains untested; and (ii) the geographic concentration of the data collected to develop the model may limit its scope of application.
Keywords: intelligence; oversight; oversight capacity; digital age.

Controle externo das atividades de inteligência na era digital: um modelo exploratório

O presente estudo desenvolve um modelo exploratório para avaliar o controle externo das atividades de inteligência em um país. Para esse fim, foi realizada uma revisão narrativa da literatura, por meio da qual foram coletadas e analisadas publicações científicas sobre esse tema. A partir daí, os elementos que caracterizam um sistema de controle externo de excelência das atividades de inteligência foram mapeados e estruturados sob a forma de um modelo de análise. O processo de criação do modelo trouxe, como resultados singulares, a clarificação do construto "capacidade de controle" e a apresentação do estado da arte da literatura científica acerca do controle externo das atividades de inteligência. O modelo proposto para avaliar o referido controle visa ser útil para estudos de caso e análises comparadas, facilitando, assim, o diagnóstico de fragilidades e subsidiando debates para sua própria melhoria. O uso do modelo objetiva proporcionar maior homogeneidade metodológica ao controle externo das

DOI: https://doi.org/10.1590/0034-761220240271x
ISSN: 1982-3134
Article submitted on August 21, 2024, and accepted for publication on April 28, 2025.
[Translated version] Note: All quotes in English translated by this article's translator.
Editor-in-chief:
Alketa Peci (Fundação Getulio Vargas, Rio de Janeiro / RJ – Brazil)
Associate editor:
Sandro Cabral (Insper Instituto de Ensino e Pesquisa, São Paulo / SP – Brazil)
Reviewers:
Francisco Wilson Ferreira da Silva (Universidade Federal do Ceará, Fortaleza / CE – Brazil)
Ricardo Rocha de Azevedo (Universidade de São Paulo, São Paulo / SP – Brazil)
Anna Carolina Mendonça Lemos Ribeiro (Instituto de Pesquisa Econômica Aplicada – Ipea, Brasília / DF – Brazil)
Peer review report:
The peer review report is available at https://periodicos.fgv.br/rap/article/view/94495/88065

atividades de inteligência na esfera digital, facilitando a compreensão global da temática, a comparação de resultados e a criação de hipóteses futuras a serem testadas. Por fim, este artigo apresenta um modelo exploratório e, portanto, ainda não testado, e a concentração geográfica dos dados obtidos pode ter limitado o alcance de sua aplicabilidade.
Palavras-chave: atividades de inteligência; controle externo; capacidade de controle; era digital.

Control externo de las actividades de inteligencia en la era digital: un modelo exploratorio

El presente estudio desarrolla un modelo exploratorio para evaluar el control externo de las actividades de inteligencia en un país. Para ello, se llevó a cabo una revisión narrativa de la literatura, mediante la cual se recopilaron y analizaron publicaciones científicas sobre el tema. Este proceso permitió mapear y estructurar los elementos que caracterizan un sistema de control externo de excelencia en forma de un modelo de análisis. Entre los principales aportes del proceso de construcción del modelo, se destacan la clarificación del constructo teórico "capacidad de control" y la presentación de los últimos avances/del nivel de desarrollo de la literatura científica sobre el control externo de las actividades de inteligencia. El modelo propuesto tiene como objetivo servir de herramienta útil para estudios de caso y análisis comparativos, lo cual facilita el diagnóstico de debilidades y respalda debates orientados a su perfeccionamiento. Se espera que el uso del modelo proporcione mayor coherencia metodológica al control externo de las actividades de inteligencia en la era digital, favoreciendo una comprensión global del tema, la comparación de resultados y la formulación de hipótesis para futuras investigaciones. Finalmente, este artículo presenta un modelo exploratorio que aún no ha sido testado, y la concentración geográfica de los datos recopilados puede limitar el alcance de su aplicabilidad.

Palabras clave: actividades de inteligencia; control externo; capacidad de control; era digital.

1. INTRODUCTION

More than a decade ago, Snowden (2019) revealed that any connected device could be transformed into a spy capable of minutely recreating and predicting an individual's routine and preferences (Parson, 2018; Zuboff, 2020; European Union [EU], 2023). Since then, the techniques employed by intelligence professionals have been significantly refined, becoming even more invasive (Xu, 2021). At present, the combination of big data, artificial intelligence (AI), cloud storage, and the internet of things—among other emerging technologies—enables any government to assemble its own "dystopia kit"[1], posing a serious threat to individual freedoms and to the very existence of democratic regimes (EU, 2023).

While the capabilities of intelligence actors have grown rapidly and consistently, progress in the oversight of their activities has failed to keep pace (Korff et al., 2017; Cayford et al., 2018; Vieth & Wetzling, 2020; Roberts et al., 2021), prompting intense debates about the urgent need for robust institutional reforms (Weinstein et al., 2017). Framed within this context, this research seeks to support both academia and policymakers in identifying more effective approaches to oversight in the digital era. In other words, this paper seeks to propose a literature-based approach for evaluating intelligence oversight systems, through the development of a framework and corresponding indicators—thus composing an exploratory model to guide such assessment.

To this end, and adopting a narrative literature review as its methodological strategy, the article explores the criteria commonly used to assess the effectiveness of intelligence external oversight systems. For this analysis, an inductive model is proposed and presented, with the aim of bringing greater coherence to the development of studies in this still underexplored area, clarifying the assumptions and steps of research on the topic, and enabling other scholars to replicate and refine the analyses conducted herein (Mershon & Shvetsova, 2019).

[1] The expression evokes the state's capacity to deploy technological apparatuses for surveillance, bringing reality closer to dystopian scenarios in which freedom is curtailed and democracy hollowed out (Zuboff, 2019).

Although research on intelligence oversight systems is not new in Brazil (Cepik, 2003; Gonçalves, 2010), it remains limited, with multiple gaps identified in the academic literature. Recent studies highlight the need to deepen our understanding of and enhance the effectiveness of intelligence oversight mechanisms in the country (Klöckner, 2023; Ribeiro, 2023). This is the research gap that the present article seeks to address.

Indeed, certain dimensions of intelligence oversight have been subject to study, such as the importance of democratic supervision (Born et al., 2015), the need to balance security and transparency (Wills & Vermeulen, 2011), and the challenges involved in implementing oversight systems (Gill & Phythian, 2018). On the other hand, several associated themes remain underexplored, including the actual impact of oversight mechanisms (Born & Wills, 2012), oversight in authoritarian and hybrid contexts (Abuza, 2016), the integration of oversight with emerging digital technologies (Chesterman, 2021), and the perspectives of stakeholders involved in oversight processes (Gill, 2016).

It is also essential to emphasize that this article focuses specifically on the external oversight of intelligence activities—distinguishing it from broader state oversight (Phythian et al., 2008). What sets the oversight of intelligence activities apart from broader state oversight is the uniquely sensitive, covert, and strategic character of these operations. These specificities demand distinct approaches and mechanisms to ensure transparency and accountability while safeguarding national security and classified information. In fact, oversight of intelligence activities is more restrictive and specialized than the general control of government. It must strike a balance between protecting sensitive information and meeting democratic demands for accountability. This type of oversight is often carried out by parliamentary committees and specialized bodies, rather than relying on the broad and public mechanisms used to supervise other government areas (Caparini, 2016).

Accordingly, the structure of this paper proceeds as follows. The next section presents the basic concepts and operational definitions used in the research. The third section outlines the methodology adopted. Sections four and five, respectively, present and discuss the proposed model. Finally, the concluding section details this study's implications—both for academia and for the formulation and evaluation of public policy—while proposing a research agenda on intelligence oversight in the digital age.

2. BASIC CONCEPTS AND OPERATIONAL DEFINITIONS

2.1. Intelligence activities

According to Gill and Phythian (2018), intelligence activities are those aimed at enhancing the security or preserving the power of an actor in relation to its competitors, by anticipating threats and opportunities. In this study, however, in order to assess the effectiveness of oversight mechanisms, a more restrictive operational definition was adopted, narrowing the scope to those activities that pose the greatest challenges to oversight — i.e., those aimed at producing political, military, and law enforcement intelligence. This group of actions, in addition to being shielded by the permissive narrative of collective security, is marked by secrecy and intrusiveness.

According to Gonçalves (2017), political intelligence supports decision-making processes at the highest levels of public administration, such as heads of government and state. Military intelligence, in turn, provides input for decision-making in the context of national defense. Law enforcement

intelligence, finally, aims to produce relevant information to guide the actions of agencies responsible for criminal investigation and repression.

Intelligence activities play a strategic role in national security, the protection of economic interests, and the formulation of public policy. However, in the digital age, these activities have undergone profound transformations driven by access to vast volumes of data, the use of emerging digital technologies, and growing global connectivity (Montasari, 2023; Polido, 2024).

Broadly speaking, intelligence activities encompass the collection, analysis, and dissemination of information to support critical decision-making in both governmental and corporate settings. These actions, traditionally reliant on human and physical sources, have evolved to include digital and automated methods, redefining the boundaries of intelligence capabilities (Khan et al., 2021).

The intelligence process consists of five main stages: planning and direction, data collection, processing, analysis and production, and dissemination (Ebell et al., 2021). The digital era, however, has brought substantial changes to each of these phases. The advent of big data has enabled the mass collection of information from diverse sources such as social networks, Internet of Things (IoT) sensors, and electronic records. This scenario has significantly expanded the data pool available for analysis, while also presenting challenges related to the filtering and management of relevant information (Ainslie et al., 2023). In addition, the use of artificial intelligence and machine learning has enabled the development of systems capable of identifying complex patterns in large datasets, predicting behavior, and anticipating threats. These technologies have enhanced the efficiency and accuracy of intelligence analysis, while reducing reliance on manual processes (Li, 2024). In short, emerging digital technologies have intensified the complexity of intelligence oversight, rendering such control all the more urgent (Pătrașcu, 2021).

Governance of intelligence activities is another fundamental aspect that demands close attention. This concept refers to the set of policies, norms, and oversight mechanisms that regulate intelligence practices, aiming to balance operational effectiveness with democratic values and human rights (Wegge, 2017). Studies suggest that transparency and accountability are essential to ensure that intelligence activities are conducted ethically and in accordance with international law (Lester, 2015). However, the complexity of the digital technologies involved and the confidential nature of such operations hinder the implementation of adequate oversight mechanisms.

In light of this, intelligence activities occupy a central role in both national and international contexts, especially in an increasingly interconnected and digitalized world (Brantly, 2020). It is therefore crucial that these practices be developed and carried out responsibly, within ethical and legal boundaries, and under a governance framework that upholds the balance between security and fundamental rights (Kniep et al., 2024). In this sense, effective oversight becomes imperative, as will be discussed below.

2.2. Intelligence oversight

Intelligence activities are typically subject to three main types of oversight: internal, external, and societal—each with specific functions aimed at ensuring the ethical, legal, and operational compliance of such actions (Caparini, 2016).

Internal oversight takes place within the intelligence agencies themselves and involves internal audits, hierarchical supervision, and codes of conduct. These mechanisms seek to ensure that

operations are aligned with institutional norms and to prevent abuses of power (Phythian et al., 2008). Moreover, specialized compliance units are tasked with ensuring that agents adhere to both internal and external regulations (Born & Wetzling, 2007).

External oversight is carried out by independent bodies such as legislative committees, the judiciary, and regulatory agencies. These mechanisms foster greater accountability by monitoring the agencies' budgets, strategies, and operations. For instance, parliaments and courts play a vital role in validating the legality of operations, thereby limiting abuses and promoting institutional transparency (Herman, 1996; Caparini, 2007).

Societal oversight, in turn, is exercised by civil society actors, such as the media, non-governmental organizations (NGOs), and citizens, who enhance scrutiny through public pressure and demands for transparency. Investigative journalism plays a critical role in exposing misconduct, while human rights organizations monitor practices that may violate civil liberties (Zuboff, 2020; Gill, 2012). Freedom of information initiatives also contribute to increasing public scrutiny of these activities (Banisar, 2006).

These three forms of oversight are complementary and essential to reconcile the operational control capacities of intelligence agencies with the protection of fundamental rights and the advancement of democratic values.

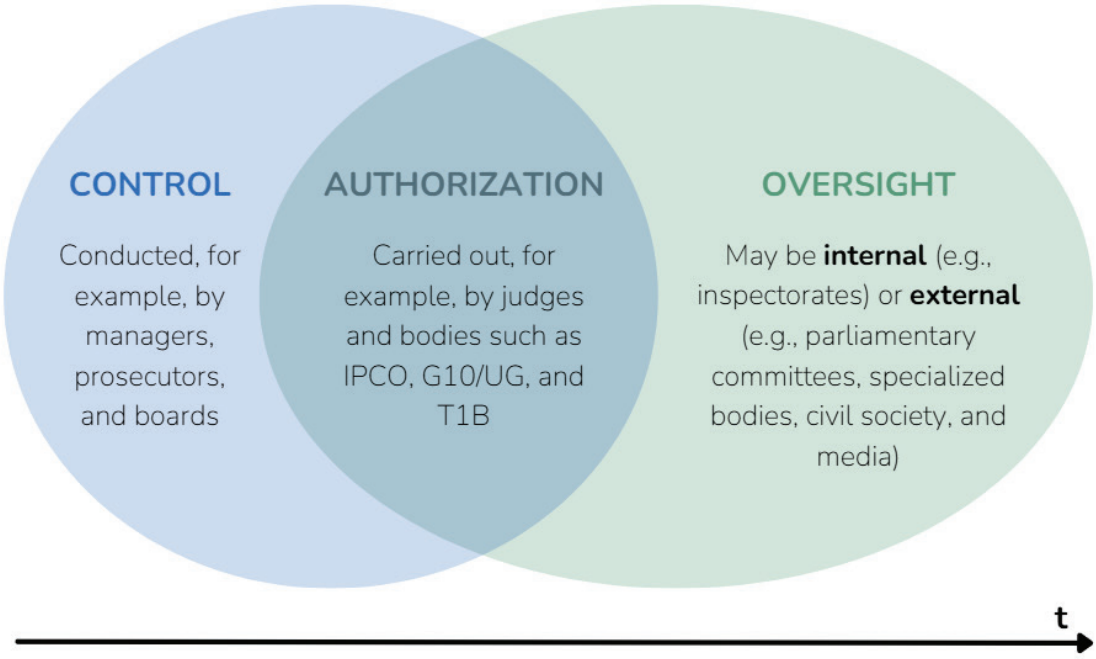
Following Gill (2020), the control of intelligence activities encompasses a range of actions that may be grouped into the stages of direction, authorization, and oversight (Figure 1). The control stage refers to the management and steering of intelligence activities. The authorization stage involves deciding whether a given activity may be carried out. Finally, oversight actions refer to the scrutiny of the efficiency, effectiveness, and compliance of these activities.

As noted, when these functions are exercised by the agency being monitored, they are considered internal oversight; when carried out by external forces, they are identified as external oversight. In political science, a force is deemed external when it originates from an organizational structure independent from that of the entity being overseen—typically involving a separate constitutional power (Meirelles, 2015), such as Parliament or the Judiciary.

The above conception by Meirelles (2015) rests on the basic premise that some formal institution is responsible for conducting the external oversight of intelligence activities—the primary focus of this study. However, in the intelligence domain, scholarly literature suggests that the concept of external oversight must be extended beyond formal institutions to include civil society[2] (societal oversight)—which, historically, has proven more effective in fulfilling this role. In this regard, scholars such as Parsons (2018), Dobson (2019), Gill (2022), and Kniep et al. (2024) argue that this inclusion is especially relevant, as real advances in intelligence accountability have largely been driven by leaks and denunciations made by whistleblowers, journalists, and activists.

[2] This includes NGOs, human rights associations, community organizations, trade unions, universities, journalists, and other actors that promote transparency, accountability, and the protection of fundamental rights in relation to State intelligence activities (Caparini & Cole, 2008).

FIGURE 1 STAGES OF INTELLIGENCE ACTIVITY CONTROL



Source: Adapted from Gill (2020, p. 972).

The next section explores how the academic literature has addressed the question of how to evaluate the effectiveness of oversight over state activities.

2.3. Measuring the effectiveness of oversight of state activities

There is no consensus on how to measure the effectiveness of oversight over state activities. According to Kinyondo et al. (2015), the literature on this subject is divided into four approaches. The first argues that effectiveness is not measurable at all, while the other three claim it can be assessed using proxy variables—namely: (1) oversight capacity, which is adopted in this study; (2) level of oversight activity; and (3) quality of institutions.

Measuring the effectiveness of oversight based on capacity means assessing whether the oversight body, if willing, has the necessary inputs to carry out its role—such as human resources and legal prerogatives. The main weakness of this approach lies in the understanding that the mere existence of such inputs does not guarantee their actual use (Pelizzo & Stapenhurst, 2012). Kinyondo et al. (2015) further argue that this approach is incapable of explaining variations in effectiveness over time in a system whose capacity remains unchanged.

The second method—based on the level of oversight activity—reflects the volume of concrete actions carried out by the oversight body (e.g., number of audits conducted). Kinyondo et al. (2015) caution that its applicability as a proxy may lead to serious inaccuracies. First, because the use of an oversight instrument is not necessarily effective. Second, because the absence of oversight activity

may, at times, indicate its very effectiveness (through deterrence), thus misleading the researcher. Furthermore, in the specific case of intelligence activities, the secrecy surrounding operational data makes this type of measurement virtually unfeasible (Dobson, 2019).

Finally, effectiveness can be measured using variables related to the quality of institutions, such as indicators of democratic robustness. The underlying logic is that effective oversight directly impacts institutional health, which can be gauged through such variables. The fundamental problem, however, is that these indicators are influenced by a wide array of factors beyond oversight systems (e.g., perceptions of corruption or voter turnout), making it scientifically unfeasible to establish a causal link between them and oversight effectiveness (Kinyondo et al., 2015). Moreover, such indicators involve highly malleable constructs that depend heavily on the subjective judgments of those who formulate them.

Thus, all the alternatives presented exhibit limitations. Nevertheless, the weaknesses associated with using "oversight capacity" as a proxy for measuring oversight effectiveness appear to be the least difficult to overcome in scientific research (Caparini, 2016). One clear advantage of this approach lies in its reliance on inputs that are, as a rule, available in public documents—a decisive factor in intelligence studies. Furthermore, it should be noted that the analysis of other variables necessarily hinges on it. In fact, capacity precedes both the oversight action itself and its potential outcomes. It is possible, for instance, that the oversight capacity granted to a body may not be used by it. However, if there is no capacity, there will certainly be no oversight action—and even less, effective oversight (Pelizzo & Stapenhurst, 2012).

3. METHODOLOGICAL PROCEDURE

This study adopted a literature review strategy aimed at developing a theoretical model to assess the external oversight capacity of intelligence activities (Paul & Criado, 2020; Post et al., 2020). Accordingly, the study employed a narrative literature review—a method chosen due to the scarcity of existing research on the topic, the need to explore theoretical concepts, the multidisciplinary nature of the field, and the constraints imposed by confidentiality (Theile & Beall, 2024). Moreover, the flexibility of narrative reviews allows for the integration of diverse information and the generation of critical analysis, thereby contributing to the advancement of knowledge in an underexplored field (Baumeister & Leary, 1997; Green et al., 2006; Grant & Booth, 2009; Ferrari, 2015).

The review drew upon three major academic databases: Scopus, Web of Science, and SSRN. Mongeon and Paul-Hus (2016) recommend using the first two for their broader coverage compared to other databases, user-friendly interfaces, bibliometric functionalities, multidisciplinary scope, and use of double-blind peer review. Similarly, Chadegani et al. (2013) endorse them for their methodological robustness, aligned with the requirements for high-quality narrative reviews. Additionally, as suggested by Veletsianos and Shepherdson (2016), scholarly articles were also retrieved from the SSRN repository—a database specialized in social sciences, economics, and law—which provides access to early-stage research and working papers. Indeed, SSRN includes studies that may not be available in traditionally indexed journals, thereby ensuring the inclusion of recent and innovative debates.

The literature review was conducted during the first quarter of 2024—following the stages proposed by Okoli and Schabram (2010)—with due flexibility allowed for narrative reviews (Siddaway et al., 2019). Its purpose was to clarify the construct "oversight capacity" and to map out the elements that

constitute an ideal oversight capacity scenario—that is, to determine what an overseer must have in order to perform their function effectively. Based on this foundation, an analytical model was developed.

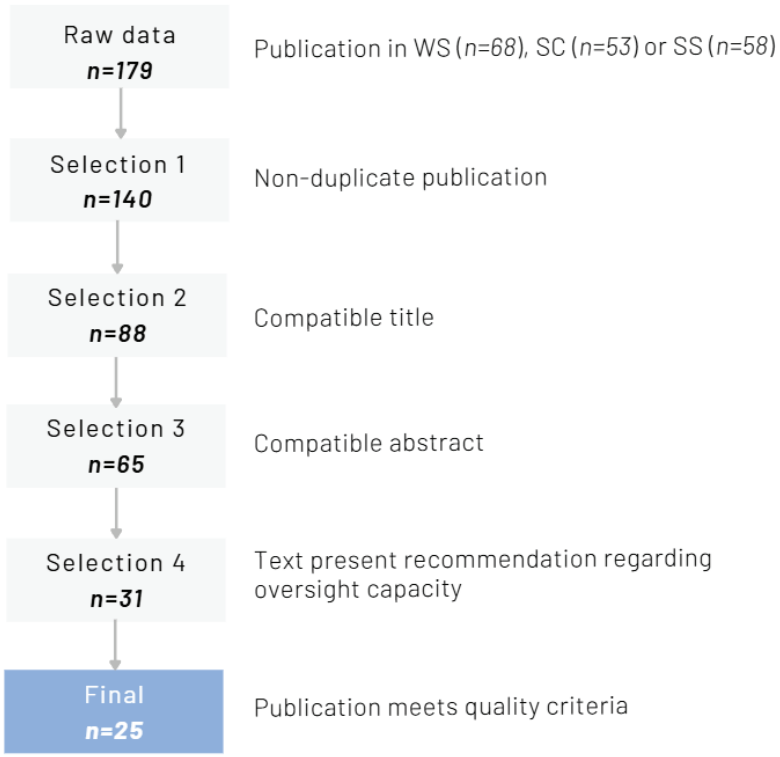
The review began with publications on intelligence oversight found through the search criteria detailed in Box 1. The data were analyzed using the principles of grounded theory, which entails a cyclical process of data collection and analysis that concludes only upon reaching theoretical saturation (Thiry-Cherques, 2009; Wolfswinkel et al., 2013). In this study, collection and analysis cycles were conducted in descending order by year, starting from 2023. That is, articles were reviewed year by year based on their titles and abstracts, and when relevant, in full text. The following year was then processed in the same manner. Upon reaching articles published before 2018, it was observed that they were increasingly scarce and largely reiterated themes already identified in more recent publications, without offering significant new insights—indicating theoretical saturation (Minayo, 2017) and prompting the conclusion of the search process. The screening procedure is detailed in Figure 2.

BOX 1 SEARCH CRITERIA

Category	Criteria
Database	Scopus, ou *Web of Science*, ou SSRN
Type of publication	Papers
Publication date	Between 2018 and 2023 (until April 1st)
Language	English
Search terms (Boolean operators) used in article titles and abstracts	"*surveillance oversight*" OR "*surveillance accountability*" OR "*surveillance regulation*" OR "*intelligence oversight*" OR "*intelligence accountability*" OR "*intelligence regulation*"

Source: Elaborated by the authors.

FIGURE 2 DATA SCREENING STAGES



Source: Elaborated by the authors.

During the data collection phase, texts were included only if their main objective was to offer specific recommendations[3] on how to improve the effectiveness of oversight systems. As a result, documents that provided only general or broad suggestions about how such systems work were excluded, as were those focused on other forms of control not related to external oversight.

The selected articles then underwent a quality screening based on two criteria: (i) having been published in blind peer-reviewed journals; or (ii) being affiliated with research institutions dedicated to the topic of intelligence oversight.

In total, 25 texts were selected, as shown in Boxes 2 and 3.

[3] In this context, "recommendations" refers to the conclusions and opinions put forward by the authors of the selected articles, in which they pointed out specific elements that positively influenced the effectiveness of an oversight system.

BOX 2 FINAL SELECTION OF PAPERS (I) – *BLIND PEER-REVIEWED*

Paper	Journal
Berman (2022)	*University of Illinois Law Review*
Bihar (2020)	*International Journal of Intelligence and CounterIntelligence*
Cahane (2020)	*International Journal of Intelligence and CounterIntelligence*
Defty (2020)	*Intelligence and National Security*
Defty (2022)	*Intelligence and National Security*
Dobson (2019)	*The British Journal of Politics and International Relations*
Duroy (2022)	*Journal of International Dispute Settlement*
Gill (2020)	*Intelligence and National Security*
Gill (2022)	*Australian Journal of Human Rights*
Gogolewska (2021)	*Connections: The Quarterly Journal*
Hillebrand (2019)	*Intelligence and National Security*
Kniep et al. (2024)	*Review of International Studies*
Krivokapić et al. (2021)	*Journal of Regional Security*
Mayer (2018)	*Yale Law Journal*
Moses (2022)	*Osgoode Hall Law Journal*
Muchwa (2021)	*Intelligence and National Security*
Obuobi (2018)	*International Journal of Intelligence and CounterIntelligence*
Van Brakel (2021)	*Surveillance & Society*
Walsh (2022)	*Intelligence and National Security*
Young et al. (2019)	*Big Data & Society*

Source: Elaborated by the authors.

BOX 3 FINAL SELECTION OF PAPERS (II) – INSTITUTIONAL PUBLICATIONS

Paper	Institution
Broeders et al. (2019)	The Hague Program for Cyber Norms
Cahane (2021)	Heinrich Böll Stiftung
Cordero and Fellow (2019)	Center for New America Security
Parsons (2018)	Citizen Lab
Vieth and Wetzling (2020)	Stiftung Neue Verantwortung

Source: Elaborated by the authors.

Data collection and analysis followed the guidelines proposed by Wolfswinkel et al. (2013). Based on a full reading of each publication, excerpts relevant to the research objective were extracted, compared, categorized, and interconnected — in a continuous coding process. Throughout this process, certain core categories emerged more prominently, providing a basis for theoretical development (Langley, 1999). In this study, as detailed in the following section, these categories were: "Autonomy Safeguards," "Powers," and "Means." The integration and refinement of these categories into a cohesive whole enabled the construction of a theoretical model for assessing the external oversight of intelligence activities.

4. MODEL FOR ASSESSING THE EXTERNAL OVERSIGHT OF INTELLIGENCE ACTIVITIES

The starting point for proposing a model to assess the external oversight of intelligence activities was the definition of oversight capacity. To this end, a two-step strategy was adopted: (1) compile excerpts from the literature review that explicitly referred to capacity; and (2) subject these excerpts to analytical comparison, seeking—through coding—to identify core categories. In Box 4, the four definitions of oversight capacity identified were broken down and coded to facilitate the identification of the core elements of this construct.

BOX 4 CODING OF DEFINITIONS OF OVERSIGHT CAPACITY

Reference	Categories comprising "oversight capacity"		
	Autonomy Safeguards	Powers	Means
Hillebrand (2019)	Political will		Resources and expertise
Vieth and Wetzling (2020)		Clear mandate	
Duroy (2022)	Independent overseer		Resources
Moses (2022)		Powers	Expertise

Source: Elaborated by the authors.

The coding process revealed that the construct "oversight capacity" comprises a set of elements that can be grouped into three core categories: autonomy safeguards, powers, and means. These categories correspond, respectively, to the volitional[4], formal, and material conditions that shape the ability to perform oversight.

Powers[5] refer to the legal tools granted to the overseer—formal authorizations for action. For these to move from potential to practice, means—that is, resources—are essential. Yet neither powers nor means are sufficient if the overseer lacks the autonomy to act. In other words, there must be institutional safeguards in place to prevent or mitigate threats to the free exercise of their mandate.

From this perspective, each of the three categories is indispensable for effective oversight. When all are in place, it can be assumed that the overseer will be able to act—if they so choose. Accordingly, oversight capacity may be defined as: "the set of autonomy safeguards, powers, and means made available to oversight agents to enable them to carry out their functions."

The study then identifies the key elements that constitute each of these three categories in a model oversight system. For clarity, these categories will be referred to as the Autonomy, Powers, and Means dimensions.

4.1. Autonomy Dimension

In order for the overseer's will to be free—and, therefore, for oversight actions to be possible—it is necessary to establish mechanisms that prevent or mitigate coercion attempts against them. Irregular intelligence activities can bring down governments, trigger diplomatic crises, and send powerful

[4] Volitional conditions represent an individual's internal state of will or disposition and are essential to explaining decisions and behaviors. That is, they pertain to a person's will, intention, or power of choice (Pires & Andrade, 2022).

[5] The term "Powers" should not be confused with the broader concept of "Power." In the context of research on oversight, "Powers" refers to external conditions — tools — granted to the overseer by the appropriate authority. Thus, within the intelligence oversight system, "Powers" pertains to the legal authority potentially conferred upon external bodies to supervise, monitor, and, when necessary, investigate the activities of intelligence services, ensuring that these bodies do not overstep the bounds of law and individual freedoms. Gill (2020) draws a clear distinction between "having powers" and "exercising power," emphasizing the importance of the political and operational context for those granted powers to translate them into effective action.

individuals to prison. It is thus only natural to presume that those responsible for investigating and prosecuting such wrongdoing will face considerable pressure (Caparini, 2016). Given that the targets of oversight are almost always political, police, or intelligence authorities—actors who are themselves experts in the use of coercion—such pressure can reach extremely high levels (Borghard & Lonergan, 2017).

Accordingly, to reduce the risk of coercion, the reviewed literature outlines a range of strategies aimed at safeguarding the autonomy of oversight agents, as presented below.

4.1.1. Regulation

The first step towards achieving autonomy lies in establishing clear regulations concerning intelligence activities and their oversight. The argument is that a fragile normative framework acts as a deterrent to the overseer. Oversight entails comparing reality to a standard (Zairi, 2010). Therefore, if that standard is unclear, or if the overseer is uncertain about the scope of their authority, any action they take will be risky. On the one hand, if the legal basis for their intervention is vague, the likelihood of impunity increases; on the other, this same legal uncertainty may lead them to fear personal retaliation. Thus, the lack of clarity fosters deterrence both through fear and through the sense of helplessness it generates.

This normative ambiguity is identified by Berman (2022) as one of the main reasons for the persistence of chronic lack of control in the field of intelligence. To address this, the literature recommends regulation that clearly delineates the powers and limits of intelligence operations and their oversight (Obuobi, 2018; Broeders et al., 2019; Gill, 2020), clarifies operational definitions (Parsons, 2018; Young et al., 2019; Berman, 2022), and precisely identifies the responsible actors (Gogolewska, 2021).

4.1.2. Traditional checks

Institutional independence between overseer and overseen is identified as a central attribute for the oversight of intelligence activities (Hillebrand, 2019; Gill, 2020). Since these activities are, as a rule, carried out by the Executive Branch, the literature recommends that their oversight be conducted by authorities from other branches, especially in emerging democracies, as is the case of Brazil (Matei & Bruneau, 2011). According to the traditional model of checks and balances, administrative oversight falls to the Parliament and the Judiciary.

Mentions of the Judiciary in the literature highlight either its typical role in reviewing the legality of administrative acts, or its specific prerogative to authorize data collection through intrusive means (Cahane, 2020; Gill, 2022; Kniep et al., 2024). Where such a power exists, it tends to be allocated to jurisdictions specialized in intelligence matters (Mayer, 2018; Cahane, 2020; Berman, 2022).

The Judiciary, being a counter-majoritarian force by design, is usually the branch most insulated from political pressure. With respect to Parliament, however, material independence is more fraught. In democratic systems, governments must build support in order to govern — a condition that renders legislatures more vulnerable in terms of autonomy.

For instance, in South Africa, Serbia, and the United States, Gill (2020) observes that parliamentary committees are generally controlled by the ruling party, which by itself tends to discourage them from undertaking actions critical of the executive. Along similar lines, in her analysis of the Polish

intelligence oversight system, Gogolewska (2021) argues that parliamentarians are reluctant to hold the government accountable, with critical expressions being rare. Likewise, in her study of Uganda's oversight system, Muchwa (2021) notes that although Parliament formally has the power to go much further, it limits itself to budgetary matters.

In a comparative study, Defty (2020) deepens this diagnosis by providing more detailed practical reasons for such executive influence. His analysis of parliamentary oversight committees in four countries — Canada, Australia, New Zealand, and the United Kingdom — concludes that all of them are controlled by the Executive. In Canada, all members are appointed by the Prime Minister; in New Zealand, the committee is chaired by the Head of Government; in Australia, the majority of members must come from the governing coalition; and in the United Kingdom, the committee can only initiate an investigation at the request of the government or of the whole legislature, which further restricts the development of an independent oversight agenda.

Given this trend of interference, the literature recommends mitigating mechanisms, which take the form either of limits on direct government participation or of guarantees for broader involvement of opposition parties. Following the first approach, Defty (2020) objects to allowing the government to select committee members or to hold seats in them. Similarly, Gogolewska (2021) criticizes the fact that the government holds the power to determine which parliamentarians may access classified material. Cordero and Fellow (2019) and Defty (2020), in turn, propose mechanisms to ensure greater participation by non-government parties, either through a minimum quota of opposition seats or by recommending that the committee be chaired by a member of the opposition.

4.1.3. Complementary checks

Another strategy highlighted in the literature involves expanding the diversity of actors engaged in the oversight front (Chesterman, 2008). The idea is to conceptualize autonomy not as an attribute of a single overseer, but rather as a feature of a broader network of external oversight. In this model, the weakness of one actor can be offset by the strength of another, ensuring the existence of alternative routes in cases of omission. This approach proves particularly relevant given the multiple limitations faced by traditional checks — namely, the Judiciary and the Parliament.

The Judiciary is naturally inert, acting only when provoked by a party with standing to invoke the law (Junior & de Quadros, 2021). In the intelligence domain, secrecy often prevents such demands from arising in the first place. Thus, within the traditional framework, a given illegality will only reach judicial scrutiny in two situations: (i) if an oversight authority empowered to monitor intelligence activities detects the illegality, or (ii) if information is leaked.

Parliament, in turn, is highly susceptible to Executive interference. Gill (2007) argues that intelligence oversight may be Parliament's greatest challenge. Hegemann (2018) and Obuobi (2018) explain that this difficulty stems from several structural peculiarities — particularly the limited electoral gains associated with intelligence oversight, since the work is confidential and any criticism is easily framed as a threat to national security.

The sections that follow present some potential complementary checks.

i) Specialized oversight

Gill (2020) argues that parliamentary control should be complemented by a specialized body. He maintains that, while elected officials possess the status and legitimacy to carry out oversight functions, they often lack the time, technical expertise, and political will to do so. These latter attributes could be supplied by a dedicated oversight body. Broeders et al. (2019) adopt a similar stance, proposing the creation of a complementary body capable of conducting investigations and reporting back to Parliament.

In his study of intelligence activities in Israel, Cahane (2020, 2021) reaches the same conclusion. Reflecting on the Israeli Parliament's role in overseeing the use of tracking technologies during the pandemic, he underscores its inability to move beyond macro-level political and legislative questions, suggesting that a complementary institution is needed to perform operational-level oversight.

Along these lines, several countries already maintain such bodies. Notable examples include the United Kingdom's Investigatory Powers Commissioner's Office (IPCO); the Netherlands' Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD, or Review Committee on the Intelligence and Security Services); and Denmark's Tilsynet med Efterretningstjenesterne (TET, or Intelligence Oversight Board).

ii) Public oversight

In cases where formal oversight mechanisms prove ineffective, some authors advocate for the possibility of public disclosure (Gill, 2022; Kniep et al., 2024). This avenue serves as a kind of last resort to safeguard the autonomy of the external oversight network. Unlike traditional reporting, which is addressed to formal institutions, public disclosure targets society directly—via the media or civil society organizations.

In support of this possibility, Kniep et al. (2024) argue that it is scandals—not institutional responses—that have historically driven oversight reform. According to the authors, it is leaks and disclosures made by whistleblowers, journalists, and activists that have exerted the pressure necessary to curb abuses committed in the name of intelligence.

This phenomenon is also noted by Parsons (2018) and Dobson (2019). As an illustrative case, Kniep et al. (2024) cite the Snowden revelations. The surveillance programs he exposed were already known to traditional oversight bodies, which were either unable or unwilling to stop them. In a recent report on the misuse of spyware, the European Union (2023) expressed concern along the same lines, underscoring the permissiveness of oversight actors.

This inaction on the part of traditional oversight is attributed to what the literature calls the "ring of secrecy"—a kind of "secrecy club." This refers to the phenomenon of closeness between overseers and those they oversee, both of whom belong to the highly restricted group with access to classified information (Kniep et al., 2024). According to this theory, personal proximity within this circle tends to discourage rigorous or confrontational interpretations, fostering a tendency toward groupthink (Duroy, 2022). Moreover, the overseer's dependency on the overseen for access to information encourages a collaborative stance. This dynamic obstructs independent verification and leads the overseer to acquiesce. Finally, the requirement of secrecy stifles the open expression of criticism (Hegemann, 2018).

An example of this phenomenon is provided by Cahane (2021) in his study on intelligence oversight in Israel. In that country, both communication data collection and wiretapping for criminal investigations are subject to ex-ante judicial control—that is, they require prior authorization. According to the author, such requests are denied in fewer than 0.5% of cases, indicating a potentially passive stance on the part of the oversight bodies.

Thus, public disclosure, according to its proponents, serves to break through these barriers of institutional inertia. In practical terms, Kniep et al. (2024) emphasize the importance of legal protections for whistleblowers. To that end, they point to the Tshwane Principles (American Civil Liberties Union [ACLU], 2013) as a legal benchmark. These principles define, for example, what types of content may be disclosed to the public and how the burden of proof should be handled.

4.2 Powers Dimension

To fulfill its functions effectively, the overseer must be equipped by law with a robust set of tools (such as the authority to conduct investigations or request information). This section addresses those tools in two parts. The first focuses on understanding their scope—that is, how far the overseer can go when exercising such prerogatives (for instance, whether a request for information could extend to intelligence operations data). The second part presents each of these tools, outlining the required mandate and the prerogatives granted.

4.2.1. Mandate

By mandate, one should understand the jurisdictional boundaries of the overseer—that is, how far they may go in exercising their prerogatives (Firmo, 2022). On this point, the literature indicates that effective oversight requires a mandate of significantly broader scope.

The first question concerns who is being overseen. Scholarship suggests that contemporary intelligence is no longer limited to traditional agencies, but extends across a vast network of stakeholders that often escape proper oversight—this includes police forces, private sector entities, and foreign actors (Gill, 2020; Moses, 2022).

With regard to police forces, Korff et al. (2017) and Bloch-Wehba (2021) highlight the growing convergence between their functions and those of traditional intelligence agencies, noting that both now operate on a similar level in terms of technical capabilities and intrusiveness. Gill (2020), in turn, draws attention to the expanding role of the private sector, which remains largely outside the reach of oversight despite supplying most of the software, equipment, and services that power contemporary intelligence.

Finally, the expansion of international cooperation has significantly increased both the risk of a country receiving intelligence obtained improperly and of its own data being used for purposes it would never permit domestically. For this reason, scholars argue that such cooperation must be subject to oversight (Broeders et al., 2019; Walsh, 2022). One example highlighted in the literature is the Netherlands, where the sharing of intelligence with foreign countries is preceded by a risk assessment conducted by the overseer itself (Gill, 2020; Vieth & Wetzling, 2020). This process makes it possible to evaluate, for instance, whether the recipient country has sufficient safeguards to prevent the misuse of shared information.

Given this expansion of the intelligence network, scholars argue that oversight mandates should be defined not institutionally, but functionally (Gill, 2020). Under the institutional model, the overseer is assigned responsibility over specific entities (e.g., the army). Under the functional model, responsibility is defined by the purpose of the activity (e.g., intelligence related to national defense). In light of the complexity of today's intelligence ecosystem, the institutional criterion is more likely to leave entire categories of activity outside the scope of oversight (Gill, 2020).

Beyond this broadening of subjective scope, the literature also recommends that oversight extends to operational activities, rather than remaining confined to macro-level domains such as regulatory or budgetary review (Matias-Pereira, 2022). Operational oversight entails monitoring intelligence work at the front line, which may include access to data from covert operations or direct access to the software used by intelligence agencies (Broeders et al., 2019).

In summary, the literature identifies the functional criterion as most appropriate for determining the subjective scope of oversight in the context of the modern intelligence network (Gonçalves, 2019; Gill, 2020). As for material scope, it emphasizes that effective oversight must "descend" to the operational level (Broeders et al., 2019; Defty, 2020; Berman, 2022).

Scholars also emphasize the need for legal safeguards to protect the mandates of oversight bodies. This means guaranteeing stable terms for their members and protecting them against arbitrary dismissal. Such safeguards are crucial to prevent political interference and to ensure consistency and continuity in the exercise of oversight functions (Born et al., 2005).

4.2.2. Prerogatives

The following section, based on a review of the literature, presents five key prerogatives that an external oversight system must possess in order to be considered effective in overseeing intelligence activities.

i) Access to information

Information is the cornerstone of effective oversight. An overseer who lacks a clear understanding of the facts cannot carry out their role (Hillebrand, 2019; Defty, 2020; Vieth & Wetzling, 2020). In a study on parliamentary oversight across four Commonwealth countries, Defty (2020) identified several limitations to this prerogative, the most significant being the prohibition of access to operational data. More broadly, he criticizes governments' recurring use of vague justifications—such as "national security"—to deny overseers access to information.

Vieth and Wetzling (2020) deepen this analysis by outlining what is needed for effective oversight of mass surveillance practices. They argue that, given the volume of data involved, oversight must be continuous and must include direct access to the operational systems of intelligence agencies. In their view, effective oversight would require, for example, algorithms capable of flagging unusual data-sharing, deletion, or search patterns. They also suggest implementing systems that link each collected data point to its prior authorization, thereby enabling auditors to assess compliance more efficiently.

These measures demand a high level of access to information, which, according to the authors, should go beyond reviewing exported databases and include full, direct access to the operational systems used by intelligence services. As a benchmark, they point to Denmark's specialized oversight body, the TET, which has full access to both operational systems and logs.

Vieth and Wetzling (2020) also emphasize that legal provisions granting access are not sufficient on their own. It is essential that the information be structured in a way that enables meaningful auditing. To achieve this, they recommend involving oversight authorities in the design phase of intelligence systems and processes. For this participation to be meaningful, they advocate the mandatory incorporation of oversight-enabling features—a principle they refer to as oversight by design[6].

ii) Budget approval

Parliamentary approval of the budget—commonly known as the "power of the purse"—is a well-established mechanism for all public expenditures, and it is hardly radical to extend this principle to intelligence activities. Cordero and Fellow (2019), however, go a step further by introducing two elements to enhance the effectiveness of this tool. The first is the allocation of budgetary authority to parliamentary committees specifically dedicated to intelligence. The second, closely linked to the first, is the recommendation that the same body responsible for approving the intelligence budget also be tasked with authorizing intelligence programs. This not only strengthens oversight but also enhances the overseer's bargaining power.

In the same vein, the oversight body should have full autonomy in preparing its own budget—meaning that no external actor should define its financial needs. This level of independence is widely regarded in the literature as essential to the effectiveness and success of intelligence oversight (Born et al., 2015).

iii) Agencies leadership approval

In democratic governments, it is common for certain strategic leadership positions not to be filled solely at the discretion of the current administration (Lopes & Vieira, 2023). One selection mechanism used to curb such discretion is subjecting the government's nominee to parliamentary scrutiny (Krause et al., 2006). Two studies included in the literature review recommend applying this practice to intelligence agencies (Obuobi, 2018; Muchwa, 2021). Both focus on oversight systems in African countries—Ghana and Uganda, respectively—where, in each case, the national parliament lacked this prerogative.

Obuobi (2018) explicitly notes that granting the Executive unrestricted authority to appoint the head of Ghana's intelligence agency renders the institution unstable and vulnerable to political capture.

iv) Authorization of intrusive actions

The idea of ex-ante oversight seeks to reduce the risk of impunity and to prevent accountability mechanisms from being triggered only after the harm has been done. This is particularly relevant in the field of intelligence, where violations can readily strike at the heart of fundamental rights and, in some cases, undermine the legitimacy—or even the existence—of democratic institutions themselves (Gill & Phythian, 2013).

[6] A set of measures designed to ensure the auditability of systems from their inception—also known as compliance by design (Moses, 2022).

In studies assessing the quality of intelligence oversight, Duroy (2022) and Gill (2020) identify the requirement for prior authorization of intrusive powers as a key indicator of effective oversight. Mayer (2018), in turn, advocates for strict ex-ante oversight particularly in cases involving real-time communications interception, which is common in contemporary intelligence practices. In support of this model, Mayer (2018) references the U.S. approach, which—through judicial precedent—requires a "super warrant" with stringent procedural safeguards for such operations.

However, while prior authorization can serve as a crucial control mechanism, it may also constrain intelligence operations—by creating delays and exposing sensitive plans that, in many cases, should remain restricted to a narrow circle of stakeholders (Gill, 2020). In this context, some scholars suggest that ex-ante authorization be granted under general rules, in order to reduce processing times and limit the risk of excessive disclosure of oversight procedures (Leigh & Wegge, 2018; Lester & Rogg, 2018).

Thus, as the literature indicates, the question of how best to structure prior authorization for intrusive intelligence actions remains open to debate.

v) Investigative powers

An investigation may involve a range of actions, such as summoning individuals to testify, breaching confidentiality, or intercepting communications. While the literature does not delve into these specifics, it consistently emphasizes that the power to conduct independent investigations is essential for effective oversight (Gill, 2020; Moses, 2022). Two studies go further, underscoring the importance of allowing overseers to initiate investigations on their own initiative, without needing external approval or provocation (Broeders et al., 2019; Defty, 2020).

A related recommendation is that of continuous monitoring, which challenges the adequacy of purely reactive investigations (Berman, 2022; Moses, 2022). Monitoring serves as a frontline safeguard, ensuring that the secrecy inherent to intelligence work does not turn into a shield for impunity. This prerogative is especially relevant in light of current technologies that enable the indiscriminate and ongoing extraction of personal data (Bajpai, 2017).

One example is the Pegasus spyware, which has been used in multiple countries to target journalists, political opponents, and activists (Kirchgaessner et al., 2021). The European Union (2023) report on the use of Pegasus notes that, unlike conventional wiretaps—where prior judicial authorization defines clear boundaries on the information that may be accessed—smartphone intrusions result in virtually unlimited and unregulated access to a target's private life. In such cases, prior authorization alone is unlikely to prevent abuse. The same applies to reactive investigations: oversight would only be effective if the overseer had the ability to continuously monitor surveillance operations. This, as Vieth and Wetzling (2020) suggest, requires direct access to the software used by intelligence agencies and to the corresponding system logs.

4.3. Means Dimension

Means refer to the human and material resources necessary for overseers to effectively exercise their prerogatives. The importance of resource adequacy is a recurring theme in the literature—sometimes as a general reference to the need for funding and staffing, and other times as a call for greater specialization among personnel (Broeders et al., 2019; Gill, 2020; Vieth & Wetzling, 2020; Duroy, 2022; Van Brakel, 2021).

Van Brakel (2021), in an analysis of intelligence oversight in Belgium, offers a compelling example of how critical resources are. Despite having the formal powers to conduct investigations, Belgian oversight bodies, in her assessment, lack the material and human conditions to carry them out. A similar situation is described by Defty (2020) in his study of parliamentary oversight in four Commonwealth countries. He finds that only in Australia did the oversight committee have its own dedicated staff. In the other three countries, human resources were supplied by the Executive—and in some cases, included personnel drawn from the intelligence agencies themselves. This arrangement, Defty concludes, compromises not only material independence but also the autonomy of the oversight process.

The link between resource sufficiency and autonomy is also emphasized by Gill (2020), who underscores the importance of having a dedicated headquarters, physically and institutionally separate from the Executive, as well as the capacity to implement secure protocols for handling classified information. Defty (2020) similarly notes the absence of a dedicated space as a shortcoming of the British parliamentary committee.

The next section details two of the most critical resources for effective oversight of intelligence activities: technical expertise and institutional specialization.

4.3.1. Expertise and institutional specialization

Contemporary intelligence involves emerging technologies whose use and comprehension demand a high level of technical expertise. For this reason, some authors go beyond general calls for human resources, refining their demands through terms such as expertise (Krivokapić et al., 2021; Van Brakel, 2021). In this vein, Moses (2022) argues that full access to data is of little value if there is no qualified personnel capable of understanding and evaluating its content.

Walsh (2022) underscores the importance of recruiting specialists in fields at the forefront of current debates, such as foreign interference, artificial intelligence, and dual-use technologies. Vieth and Wetzling (2020) contend that oversight authorities must be equipped—at a minimum—with technological capabilities that match those of the agencies they monitor. Expertise, they argue, is essential for enabling overseers to operate independently from both external consultants and the intelligence agencies themselves.

In parallel, part of the academic literature suggests that intelligence oversight should be carried out by actors specifically established for that purpose, with exclusive focus on this function. In the Ghanaian Parliament, for instance, Obuobi (2018) identifies as a weakness the fact that intelligence matters are handled by a generic defense and interior committee operating on a part-time basis. Other authors go further, advocating for the creation of a new, independent, and complementary body devoted exclusively to intelligence oversight (Cahane, 2020; Gill, 2020).

4.4. Analytical model

The findings from the literature review provide the foundation for constructing an analytical model to assess external oversight of intelligence activities, based on the consolidation of three dimensions and seven analytical elements. This model is built on the following premises:

a) state actions that escape external oversight constitute potential spaces for abuse of power, in line with the theory of checks and balances (Lowenstein, 1979);

b) oversight capacity is a necessary precondition for oversight to exist (Pelizzo & Stapenhurst, 2012);

c) oversight capacity is a suitable proxy variable for evaluating the effectiveness of intelligence oversight;

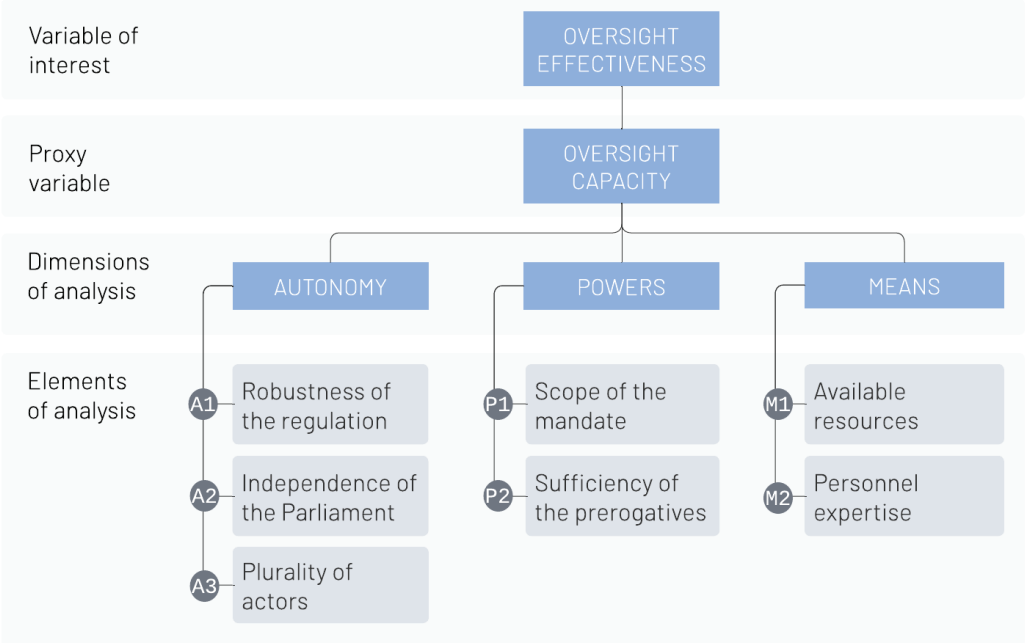
d) oversight capacity can be understood as the combination of autonomy safeguards, powers, and means granted to the oversight body to enable it to perform its functions;

e) each of the three dimensions of oversight capacity—autonomy, powers, and means—is, on its own, a necessary condition for oversight capacity to exist;

f) taken together, the three dimensions constitute a sufficient condition for the existence of oversight capacity.

Based on this logical framework, the recommendations identified in the literature have been organized into a model—that is, a logical and functional structure designed to facilitate future analysis and evaluation of external oversight over intelligence activities (Figure 3).

FIGURE 3 PROPOSED ANALYTICAL MODEL



Source: Elaborated by the authors.

The analytical elements within each dimension have been structured to allow for sectoral analysis and the grouping of potential indicators. As such, both the dimensions and their corresponding analytical elements can be interpreted as variables within the proposed model. Future studies may choose to translate these variables into measurable indicators.

To lay the groundwork for this operationalization, the set of recommendations drawn from the reviewed literature has been organized into a list of analytical criteria, each linked to one of the seven elements of the model, as outlined in Box 5.

BOX 5 ANALYTICAL CRITERIA FOR EACH ELEMENT OF THE MODEL

A1	Robustness of the regulation	References
A1.1	Regulation of the intelligence activities	Parsons (2018); Broeders et al. (2019); Young et al. (2019); Gill (2020); Gogolewska (2021); Krivokapić et al. (2021); Berman (2022)
	1) has the status of law	
	2) details actors, mandate, purposes, powers and their limits	
A1.2	Regulation of the intelligence oversight	Obuobi (2018); Gill (2020)
	1) has the status of law	
	2) details actors, mandate, purposes, powers and their limits	
A2	**Independence of the Parliament**	**References**
A2.1	There is a specific commission for intelligence oversight	Cordero and Fellow (2019); Defty (2020)
A2.2	Parliamentary commission that oversights intelligence has rules for:	Cordero and Fellow (2019); Defty (2020)
	1) banning government members from membership;	
	2) guaranteeing multiparty composition;	
	3) guaranteeing the opposition the power to choose or veto the presidency.	
A3	**Plurality of actors**	**References**
A3.1	There is a specific judicial unit for demands related to intelligence oversight	Mayer (2018); Cahane (2020); Berman (2022)
A3.2	There is an independent and specialized intelligence oversight body, separate from the Executive, which serves a complementary oversight role alongside the Parliament and Judiciary	Broeders et al. (2019); Cahane (2020); Gill (2020); Cahane (2021)
A3.3	There is a legal protection system for public complaints about misconduct within the intelligence community	Gill (2022); Kniep et al. (2024)

(Continue)

P1	Scope of the mandate	References
P1.1	Scope of mandate reach activities at operational level	Broeders et al. (2019); Defty (2020); Berman (2022)
P1.2	Scope of mandate is determined by the purpose of the intelligence activity rather than by the entity carrying it out (primacy of functional approach)	Gill (2020); Moses (2022)
P1.3	Scope of mandate encompasses intelligence activities with the purpose of national security and defense, public safety and criminal investigation	Gill (2020); Moses (2022)

P2	Sufficiency of the prerogatives	References
P2.1	Overseer has the authority to access all information held by the overseen entities and the companies that provide services to them, including: 1) direct access to software, operating systems, and their associated logs and source codes; 2) access to information obtained through international cooperation; 3) access to physical facilities.	Obuobi (2018); Broeders et al. (2019); Hillebrand (2019); Defty (2020); Gill (2020); Vieth and Wetzling (2020); Duroy (2022); Moses (2022); Kniep et al. (2024)
P2.2	Overseer can determine changes to systems and processes considered unauditable	Vieth and Wetzling (2020)
P2.3	Overseer decides whether a member of its staff receives security clearance	Gogolewska (2021)
P2.4	Overseer must approve the nomination of the heads of intelligence agencies	Obuobi (2018); Muchwa (2021)
P2.5	Overseer approves the intelligence budget	Born and Leigh (2015); Cordero and Fellow (2019)
P2.6	Overseer has the power to previously authorize data collection by intrusive means	Mayer (2018); Cahane (2020); Gill (2020); Duroy (2022); Berman (2022)
P2.7	Overseer can initiate and undertake investigations to assess the legality of intelligence activities	Broeders et al. (2019); Hillebrand (2019); Defty (2020); Gill (2020); Moses (2022)
P2.8	Overseer can undertake continuous monitoring	Born et al. (2005); Born et al. (2015); Vieth and Wetzling (2020); Berman (2022); Moses (2022)

(Continue)

M1	Available resources	References
M1.1	Overseer has material, financial and human resources compatible with its duties	Broeders et al. (2019); Gill (2020); Vieth and Wetzling (2020); Duroy (2022); Van Brakel (2021)
M2	**Personnel expertise**	**References**
M2.1	Level of expertise of overseers is at least equivalent to that of overseen bodies	Hillebrand (2019); Cahane (2020); Gill (2020); Vieth and Wetzling (2020); Cahane (2021); Krivokapić et al. (2021); Van Brakel (2021); Berman (2022); Moses (2022)

Note: A = Autonomy Dimension; P = Powers Dimension; M = Means Dimension.

Source: Elaborated by the authors.

The list of criteria presented reflects all the recommendations identified in the literature review. The decision to include them in full in Box 5 is grounded in the need to ensure that, at this early stage, the proposed model remains a flexible tool for exploration (Mershon & Shvetsova, 2019). The aim, after all, is not to construct an exact mirror of reality, but to facilitate a clearer understanding of the phenomenon under study (Shoemaker et al., 2004).

5. DISCUSSION

The literature shows that the current state of intelligence activities is marked by a serious lack of control, making institutional reform agendas aimed at strengthening oversight urgent (Weinstein et al., 2017; Gill, 2020). The review conducted suggests that research focused on assessing oversight capacity can offer valuable input for these reform efforts. Typically, such studies aim to evaluate whether oversight actors possess the necessary conditions to fulfill their roles. As a result, they yield diagnoses with potential relevance for both policymakers and scholars.

However, this body of work suffers from a lack of methodological consistency. In fact, the criteria and categories of analysis used vary considerably from one author to another. This inconsistency hampers not only the development of new research in the field but also the comparability of findings, the overall understanding of the topic, the generation of hypotheses, and the translation of academic insights into public policy.

Obuobi (2018), for example, sets out to assess the effectiveness of Ghana's oversight system. However, his article does not specify any analytical criteria, offering instead a descriptive account of the institutions involved, followed by an evaluation disconnected from a theoretical framework capable of justifying the conclusions and methodological choices. One trend that reinforces this weakness is the predominance of studies focusing on only part of the oversight system. Defty (2020), for instance, examines only one oversight actor—Parliament—while Moses (2022) addresses only one of the entities being overseen—the police. Although both are comparative studies covering nearly the same set of countries, the absence of a shared analytical grammar makes it difficult to compare their results in a coherent manner.

As a consequence, a researcher or policymaker seeking to assess the oversight capacity of institutions in their country may struggle to determine where to look or which standard to apply. The

model proposed here aims to fill that gap and, in doing so, help establish a basic foundation for the advancement of research in the field of intelligence oversight. Its structure is particularly well-suited to case studies and comparative analyses—especially when the objective is to diagnose weaknesses in external oversight systems.

That said, two important limitations of the model's applicability must be considered:

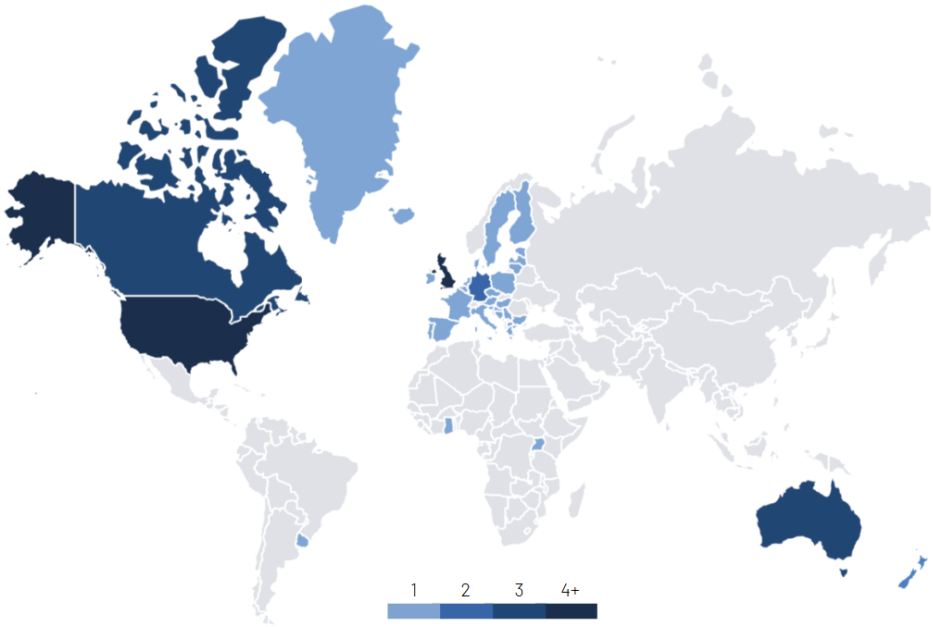
(1) the model was designed to facilitate the analysis of the oversight system as a whole, not of individual oversight bodies in isolation; and

(2) the analytical elements and criteria are drawn primarily from studies of institutions in Western democracies, which may limit the model's applicability in other contexts.

Regarding the first point, the model is grounded in the understanding that both intelligence activity and its oversight are diffuse, and that analyzing institutions in isolation yields little value. Take, for example, the analytical element "scope of mandate", which requires examining whether the collective mandate of oversight bodies covers all intelligence activities. It may be the case that gaps in parliamentary oversight are offset by the prerogatives of a judicial authority—but this would only be evident through a joint institutional analysis. Therefore, the only form of disaggregation offered by the model is by dimension or analytical element—with the full oversight system as the underlying unit of analysis. For instance, one could compare countries based on whether their oversight systems possess sufficient prerogatives—analytical element P2 in the proposed model (see Box 5 for further detail).

As for the second point, it is important to recognize the contextual limits of the model, stemming from the nature of the literature on which it is based. The majority of the studies reviewed focus on oversight systems in developed Western countries, particularly in the Anglo-Saxon world, which accounts for 53% of the publications—a trend already noted in the literature (Defty, 2020; Kniep et al., 2024). In contrast, studies centered on the Global South represent only 12% of the references collected. Figure 4 illustrates the extent of this concentration.

FIGURE 4 FREQUENCY OF COUNTRIES AS OBJECTS OF STUDY IN THE REVIEW



Frequency: (1) Austria, Belgium, Bosnia and Herzegovina, Croatia, Slovenia, Ghana, North Macedonia, Poland, Serbia, Uganda, European Union, Uruguay; (2) Germany, Israel, New Zealand; (3) Australia, Canada; (4) United Kingdom; (5) United States.

Source: Elaborated by the authors.

Therefore, when applying the proposed model in political systems that differ from the typical patterns of Western democracies, it is important to approach its analytical elements and criteria with care, taking into account cultural and institutional variations (Davison & Martinsons, 2016). That said, this limitation should not be seen as an obstacle to using the findings of this study. As an exploratory tool still in its early stages, the model is meant to be flexible — open to adaptation and refinement as new evidence becomes available.

6. CONCLUSIONS

The literature review revealed a certain degree of methodological dissonance among academic studies addressing the external oversight of intelligence activities. This lack of consistency hinders a comprehensive understanding of the field, the comparability of findings, and the development of testable hypotheses. In response, the present study seeks to help close that gap by mapping the state of the art in the existing literature and offering, through an exploratory model, a conceptual framework that enables more theoretically cohesive research on the topic. In doing so, the model paves the way for more harmonized studies that can advance scientific development in this still underexplored area.

It is evident that new surveillance technologies are highly invasive and difficult to control, posing serious risks to both the legitimacy and the very survival of democratic institutions (Prince et al.,

2021; Zuboff, 2022). Aware of these risks, many countries have begun to pursue stronger oversight mechanisms for intelligence activities, which in turn demands meaningful reform of existing structures. However, achieving this requires both sound diagnostics and the exploration of viable alternatives.

The model proposed here is designed to support both efforts. On one hand, it offers a detailed roadmap for diagnosing weaknesses in external oversight systems, classifying those weaknesses and indicating how each may impact overall oversight capacity. On the other hand, it contributes to the search for solutions, as the standardization of analytical categories makes it easier to conduct comparative studies and identify potential benchmarks.

6.1. Theoretical and methodological limitations

This study presents a number of theoretical and methodological limitations, outlined below. The primary limitation concerns the use of the construct "oversight capacity" as a proxy for evaluating the effectiveness of intelligence oversight. While oversight capacity—understood here as the combination of Autonomy, Powers, and Resources—is essential, it does not in itself guarantee effective oversight. Other factors, such as the political will to act, also play a crucial role in determining the overall effectiveness of the system (Born et al., 2015).

Moreover, although oversight capacity is a structural variable that is often measurable, its effectiveness also depends on qualitative factors—such as the extent to which oversight actions reduce abuses, promote transparency, and strengthen accountability. These indicators may not always be immediately visible or quantifiable (Gill, 2020). In addition, even when oversight institutions possess high capacity, they may still become politically captured or ineffective due to conflicts of interest or deliberate inaction (Caparini, 2016). Therefore, formal oversight capacity does not necessarily reflect how external oversight functions in practice.

A second theoretical-methodological limitation lies in the fact that the proposed model has not yet been empirically tested. As such, adjustments to its current configuration may be required once it is applied in practice. Nonetheless, it is important to acknowledge the inherent challenges of conducting empirical research on national intelligence oversight systems (Gioe et al., 2020). Testing the proposed model is, therefore, not a straightforward undertaking.

Furthermore, this study assumes that the three core dimensions of the proposed model—Autonomy, Powers, and Resources—are linearly independent. In reality, this may not always hold true, as there could be areas of overlap among these dimensions in certain assessments (Child & Rodrigues, 2011).

Despite these limitations, it is recommended that the exploratory model developed in this study be tested in diverse contexts—particularly those not covered by the literature review, with special attention to the Global South. In the process of testing, it would be valuable to examine the correlations between different dimensions, elements, and analytical criteria. A correlation map of these relationships could serve as an important tool in identifying strategic pathways for institutional reform aimed at strengthening external intelligence oversight.

6.2. Future steps

The model draws heavily from academic literature produced in developed countries, as illustrated in Figure 4. However, the socioeconomic, political, and institutional context of each country plays

a significant role in shaping how external oversight of intelligence activities operates (Davison & Martinsons, 2016). National context directly influences the levels of accountability, transparency, and effectiveness of intelligence oversight mechanisms, affecting how they are implemented and enforced (Caparini, 2016). Still, the methodological approach adopted here remains justified, as the aim was to identify best practices in external intelligence oversight—thereby allowing an assessment of how close or far a country like Brazil is from achieving effective oversight. In other words, the institutional context does not change the proposed model; it merely reveals how easy or difficult it is to implement effective oversight in a given country.

With that in mind, several future research directions can be envisioned, as outlined below:

i) Empirical testing of the model: The model should be tested across different countries, including both consolidated and emerging democracies, and in various oversight settings (e.g., judiciary, parliament, civil society). Such testing would help validate the model's robustness, identify necessary adjustments, and generate empirical data to further refine the framework.

ii) Expanding geographic and contextual scope: While this study acknowledges that the proposed model is rooted in literature from Western democracies, future research should broaden the analysis to include more Global South countries, where oversight systems and intelligence practices may differ significantly. Including countries with diverse political and cultural contexts could help develop a more global and adaptable model, fostering a more inclusive and pluralistic perspective on intelligence oversight.

iii) Deepening the discussion on emerging technologies: Although the paper touches on the increasing complexity of technologies used in intelligence—such as big data, AI, and digital surveillance—a more detailed analysis of how these tools can both enable and hinder oversight (e.g., through automated monitoring or misuse of personal data) would enrich the theoretical and practical discussion.

iv) Further exploration of oversight autonomy: The model highlights the importance of autonomy for oversight bodies, but this dimension could be explored in greater depth in future studies. This includes examining specific strategies to safeguard institutional independence and analyzing how the relationships between overseers and those they oversee can be structured to avoid conflicts of interest.

v) Development of indicators: Creating a set of measurable indicators would help transform the model into a practical tool for researchers, policymakers, and civil society organizations aiming to assess the effectiveness of external intelligence oversight.

vi) Engagement with civil society and transparency: Future work could strengthen the model by incorporating a deeper discussion of the role of civil society in intelligence oversight. Mechanisms such as whistleblower channels, NGO monitoring, and media transparency are valuable components that can complement institutional control.

vii) Ethical and human rights considerations: Including a more robust analysis of the ethical implications of personal data use and invasive surveillance practices would be a meaningful

addition, as intelligence activities often raise sensitive issues related to privacy and individual freedoms.

viii) Critical reflection on the role of government: Future articles could offer a more critical reflection on the role of government in intelligence oversight. In many democracies, the Executive may have a vested interest in limiting transparency or avoiding scrutiny that could undermine its image or policies.

ix) Expert validation of the model: The proposed model could be further refined by submitting it to expert review. A Delphi study, for example, could enhance the validity of the model's findings—especially if it helps identify additional criteria that are crucial for effective external oversight of intelligence activities.

In sum, despite the many future directions outlined above, it is hoped that the study and the exploratory model presented here will serve as useful tools for academics, practitioners, and policymakers seeking to better understand and strengthen external intelligence oversight—particularly in light of emerging digital technologies and their far-reaching implications.

REFERENCES

Abuza, Z. (2016). *Forging peace in Southeast Asia: Insurgencies, peace processes, and reconciliation*. Rowman & Littlefield.

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, *132*, 103352. https://doi.org/10.1016/j.cose.2023.103352

American Civil Liberties Union. (2013). *The global principles on national security and the right to information (Tshwane principles)*. Open Society Foundations. https://www.aclu.org/documents/global-principles-national-security-and-right-information-tshwane-principles

Bajpai, D. (2017). The collection without permission: WhatsApp's data sharing policy. *Supremo Amicus, 2*(1), 139. https://heinonline.org/HOL/LandingPage?handle=hein.journals/supami2&div=19

Banisar, D. (2006). The right to information in the age of information. In R. F. Jørgensen (Ed.). *Human rights in the global information society* (pp. 77–89). MIT Press. https://doi.org/10.7551/mitpress/3606.003.0005

Baumeister, R. F., & Leary, M. R. (1997). Writing narrative literature reviews. *Review of General Psychology, 1*(3), 311–320. https://doi.org/10.1037/1089-2680.1.3.311

Berman, E. (2022). Reimagining surveillance law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4161996

Bihar, A. M. (2020). Uruguay's attempt at intelligence oversight. *International Journal of Intelligence and CounterIntelligence, 33*(2), 214–247. https://doi.org/10.1080/08850607.2019.1663701

Bloch-Wehba, H. (2021). Visible policing: technology, transparency, and democratic control. *California Law Review*, 109(3), 917–978. https://doi.org/10.15779/Z38NSOKZ51

Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies, 26*(3), 452–481. https://doi.org/10.1080/09636412.2017.1306396

Born, H., Johnson, L. K., & Leigh, I. (2005). *Who's watching the spies? Establishing intelligence service accountability*. Potomac Books.

Born, H., Leigh, I., & Wills, A. (2015). *Making international intelligence cooperation accountable*. Printing Office of the Parliament of Norway.

Born, H., & Wetzling, T. (2007). Intelligence accountability: challenges for parliaments and intelligence services. In *Handbook of intelligence studies* (pp. 315–328). Routledge.

Born, H., & Wills, A. (2012). *Overseeing intelligence services: A toolkit*. DCAF.

Brantly, A. F. (2020). When everything becomes intelligence: machine learning and the connected world. In *Developing Intelligence Theory* (pp. 96-107). Routledge.

Broeders, D., Boeke, S., & Georgieva, I. (2019). *Foreign intelligence in the digital age: Navigating a state of "Unpeace"*. SSRN. https://papers.ssrn.com/abstract=3493612

Cahane, A. (2020). Who will watch the watchmen? Oversight of online surveillance in Israel. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3819815

Cahane, A. (2021). The (missed) Israeli Snowden moment? *International Journal of Intelligence and CounterIntelligence, 34*(4), 694–717. https://doi.org/10.1080/08850607.2020.1838902

Caparini, M. (2007). Domestic regulation: Licensing regimes for the export of military goods and services. In S. Chesterman & C. Lehnardt (Eds.). *From mercenaries to market: the rise and regulation of private military companies* (pp. 158–178). Oxford. https://doi.org/10.1093/acprof:oso/9780199228485.003.0010

Caparini, M. (2016). Controlling and overseeing intelligence services in democratic states. In H. Born & M. Caparini (Eds.), *Democratic control of intelligence services* (pp. 3–24). Routledge. https://doi.org/10.4324/9781315576442

Caparini, M., & Cole, E. (2008). The case for public oversight of the security sector: Concepts and strategies. In *Public oversight of the security sector: A handbook for civil society organizations* (pp. 11–30). DCAF.

Cayford, M., Pieters, W., & Hijzen, C. (2018). Plots, murders, and money: Oversight bodies evaluating the effectiveness of surveillance technology. *Intelligence and National Security, 33*(7), 999–1021. https://doi.org/10.1080/02684527.2018.1487159

Cepik, M. (2003). Sistemas nacionais de inteligência: origens, lógica de expansão e configuração atual. *Dados, 46*, 75–127. https://doi.org/10.1590/S0011-52582003000100003

Chadegani, A. A., Salehi, H., Yunus, M. M., Farhadi, H., Fooladi, M., Farhadi, M., & Ale Ebrahim, N. (2013). A comparison between two main academic literature collections: Web of Science and Scopus databases. *Asian Social Science*, *9*(5), 18–26. https://doi.org/10.48550/arXiv.1305.0377

Chesterman, S. (2008). We can't spy... if we can't buy!: The privatization of intelligence and the limits of outsourcing "inherently governmental functions". *European Journal of International Law, 19*(5), 10551074. https://doi.org/10.1093/ejil/chn055

Chesterman, S. (2021). *We, the robots?* Cambridge University Press. https://doi.org/10.1017/9781009047081

Child, J., & Rodrigues, S. B. (2011). How Organizations Engage with External Complexity: A Political Action Perspective. *Organization Studies*, 32(6), 803–824. https://doi.org/10.1177/0170840611410825

Cordero, C., Fellow, R. M. G. S. (2019). *Working paper : Enhancing congressional intelligence committee effectiveness*. Center for a New American Security. https://doi.org/10.2139/ssrn.3454315

Davison, R. M., & Martinsons, M. G. (2016). Context is king! Considering particularism in research design and reporting. *Journal of Information Technology, 31*, 241–249. https://doi.org/10.1057/jit.2015.19

Defty, A. (2020). From committees of parliamentarians to parliamentary committees: Comparing intelligence oversight reform in Australia, Canada, New Zealand and the UK. *Intelligence and National Security, 35*(3), 367–384. https://doi.org/10.1080/02684527.2020.1732646

Defty, A. (2022). 'Familiar but not intimate': executive oversight of the UK intelligence and security agencies. Intelligence and National Security, 37(1), 57–72. https://doi.org/10.1080/02684527.2021.1959697

Dobson, M. J. (2019). The last forum of accountability? State secrecy, intelligence and freedom of information in the United Kingdom. *The British Journal of Politics and International Relations, 21*(2), 312–329. https://doi.org/10.1177/1369148118806125

Duroy, S. (2022). State compliance with international law in intelligence matters: A behavioral approach. *Journal of International Dispute Settlement, 13*(2), 233–263. https://doi.org/10.1093/jnlids/idab029

Ebell, C., Baeza-Yates, R., Benjamins, R., Cai, H., Coeckelbergh, M., Duarte, T., Hickok, M., Jacquet, A., Kim, A., Krijger, J., MacIntyre, J., Madhamshettiwar, P., Maffeo, L., Matthews, J., Medsker, L., Smith, P., & Thais, S. (2021). Towards intellectual freedom in an AI Ethics Global Community. *AI and Ethics*, *1*, 131–138. https://doi.org/10.1007/s43681-021-00052-5

Ferrari, R. (2015). Writing narrative style literature reviews. *Medical Writing, 24*(4), 230–235. https://doi.org/10.1179/2047480615Z.000000000329

Firmo, M. R. (2022). Limites éticos da atividade de inteligência. *Revista Ciência & Polícia, 8*(2), 36–50. https://doi.org/10.59633/2316-8765.2022.252

Gill, P. (2007). Evaluating intelligence oversight committees: The UK Intelligence and Security Committee and the 'war on terror'. *Intelligence and National Security*, 22(1), 14–37. http://dx.doi.org/10.1080/02684520701200756

Gill, P. (2012). *Policing politics: security intelligence and the liberal democratic state*. Routledge. https://doi.org/10.4324/9780203043776

Gill, P. (2016). *Intelligence governance and democratisation: A comparative analysis of the limits of reform*. Routledge.

Gill, P. (2020). Of intelligence oversight and the challenge of surveillance corporatism. *Intelligence and National Security, 35*(7), 970–989. https://doi.org/10.1080/02684527.2020.1783875

Gill, P. (2022). Intelligence, oversight and the ethics of whistleblowing: The case of Witness K. *Australian Journal of Human Rights, 28*(2/3), 206–224. https://doi.org/10.1080/1323238X.2022.2145834

Gill, P., & Phythian, M. (2013). *Intelligence in an insecure world* (2nd ed.). Wiley.

Gill, P., & Phythian, M. (2018). Developing intelligence theory. *Intelligence and National Security*, *33*(4), 467–471. https://doi.org/10.1080/02684527.2018.1457752

Gioe, D. V., Goodman, M. S., & Stevens, T. (2020). Intelligence in the cyber era: Evolution or revolution? *Political Science Quarterly, 135*(2), 191–224. https://doi.org/10.1002/polq.13031

Gogolewska, A. (2021). Transformation of state security and intelligence services in Poland — A job still unfinished. *Connections: The Quarterly Journal, 20*(1), 9–32. https://doi.org/10.11610/Connections.20.1.01

Gonçalves, J. B. (2010). Quem vigia os vigilantes? O controle da atividade de inteligência no Brasil e o papel do Poder Legislativo. *Revista de Informação Legislativa, 47*(187), 125–136. http://www2.senado.leg.br/bdsf/handle/id/496919

Gonçalves, J. B. (2017). *Atividade de inteligência e legislação correlata* (5th ed.). Impetus.

Gonçalves, J. B. (2019). *Políticos e espiões: O controle da atividade de inteligência* (2nd ed.). Impetus.

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal, 26*(2), 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing narrative literature reviews for peer-reviewed journals: Secrets of the trade. *Journal of Chiropractic Medicine, 5*(3), 101–117. https://doi.org/10.1016/S0899-3467(07)60142-6

Hegemann, H. (2018). Toward 'normal' politics? Security, parliaments and the politicisation of intelligence oversight in the German Bundestag. *The British Journal of Politics and International Relations*, 20(1), 175–190. https://doi.org/10.1177/1369148117745683

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge University Press. https://doi.org/10.1017/CBO9780511521737

Hillebrand, C. (2012). The role of news media in intelligence oversight. In R. Dover, H. Dylan, & M. S. Goodman (Eds.). A Decade of Intelligence Beyond 9/11: Security, Diplomacy and Human Rights (pp. 689-706). *Intelligence and National Security, 27*(5). https://doi.org/10.1080/02684527.2012.708521

Hillebrand, C. (2019). Placebo scrutiny? Far-right extremism and intelligence accountability in Germany. *Intelligence and National Security, 34*(1), 38–61. https://doi.org/10.1080/02684527.2018.1540175

Junior, É., & de Quadros, D. (2021). A constituição como limite para o ativismo do Judiciário. *Revista Brasileira de Teoria Constitucional*, 7(2), 73–88. https://doi.org/10.26668/IndexLawJournals/2525-961X/2021.v7i2.8274

Keane, J. (2009). *The life and death of democracy*. W. W. Norton & Company.

Khan, A., Imam, I., & Azam, A. (2021). Role of Artificial Intelligence in Defence Strategy. *Strategic Studies*, *41*(1), 19–40. https://doi.org/10.53532/ss.041.01.0058

Kinyondo, A., Pelizzo, R., & Umar, A. (2015). A functionalist theory of oversight. *African Politics & Policy, 1*(5), 1–25. https://www.researchgate.net/profile/Riccardo-Pelizzo-2/publication/292227902_A_Functionalist_Theory_of_Oversight/links/56ac376808ae19a385116801/A-Functionalist-Theory-of-Oversight.pdf

Kirchgaessner, S., Cutler, S., Pegg, D., & Sabbagh, D. (2021, July 18). *Revealed: Leak uncovers global abuse of cyber-surveillance weapon*. The Guardian. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

Klöckner, C. (2023). *A capacidade de controle externo das atividades de inteligência na era digital* [Dissertação de mestrado]. Fundação Getulio Vargas. https://repositorio.fgv.br/items/af86cd33-d297-4465-8d12-4a27634e4899

Kniep, R., Ewert, L., Reyes, B. L., Tréguer, F., Mc Cluskey, E., & Aradau, C. (2024). Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies*, *50*(1), 209–229. https://doi.org/10.1017/S0260210523000013

Korff, D., Brown, I., & Wright, J. (2017). *Boundaries of law: Exploring transparency, accountability, and oversight of government surveillance regimes*. Cambridge Legal Studies Research. https://papers.ssrn.com/abstract=2894490

Krause, G., Lewis, D., & Douglas, J. (2006). Political Appointments, Civil Service Systems, and Bureaucratic Competence: Organizational Balancing and Executive Branch Revenue Forecasts in the American States. *American Journal of Political Science*, 50(3), 770–787. http://www.jstor.org/stable/3694248

Krivokapić, Đ., Krivokapić, D., Adamović, J., & Stefanović, A. (2021). Comparative analysis of video surveillance regulation in data protection laws in the former Yugoslav states. *Journal of Regional Security, 16*(1), 5-26. https://doi.org/10.5937/jrs16-27170

Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management Review, 24*(4), 691–710. https://doi.org/10.2307/259349

Leigh, I., & Wegge, N. (2018). Intelligence and oversight at the outset of the twenty-first century. In *Intelligence Oversight in the Twenty-First Century* (pp. 7–24). Routledge. https://doi.org/10.4324/9781351188791

Lester, G. (2015). *When should state secrets stay secret?: accountability, democratic governance, and intelligence*. Cambridge University Press. https://doi.org/10.1017/CBO9781107337015

Lester, G., & Rogg, J. (2018). Intelligence and oversight. In I. Leigh & N. Wegge. *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*. Routledge.

Li, Z. (2024). Ethical frontiers in artificial intelligence: navigating the complexities of bias, privacy, and accountability. *International Journal of Engineering and Management Research*, *14*(3), 109–116. https://doi.org/10.5281/zenodo.12792741

Lopes, A., & Vieira, D. (2023). Between politics and bureaucracy: a systematic literature review on the dynamics of public appointments. *International Journal of Public Sector Management*, 36(2), 152–170. https://doi.org/10.1108/IJPSM-09-2022-0200

Lowenstein, K. (1979). *Teoría de la Constitución* (2nd ed.). Ariel.

Matei, F. C., & Bruneau, T. (2011). Intelligence reform in new democracies: Factors supporting or arresting progress. *Democratization, 18*(3), 602–630. http://dx.doi.org/10.1080/13510347.2011.586257

Matias-Pereira, J. (2022). Governance in the public sector: Emphasis on better management, transparency and society participation. *Brazilian Journal of Development, 8*(9), 63172–63195. https://doi.org/10.34117/bjdv8n9-183

Mayer, J. (2018). Government hacking. *Yale Law Journal, 127*(3), 490–787. https://www.yalelawjournal.org/article/government-hacking

Meirelles, H. L. (2015). *Direito administrativo brasileiro* (42a ed.). Malheiros.

Mershon, C., & Shvetsova, O. (2019). *Formal modeling in social science*. University of Michigan Press.

Minayo, M. C. S. (2017). Amostragem e saturação em pesquisa qualitativa: Consensos e controvérsias. *Revista Pesquisa Qualitativa, 5*(7), 1–12. https://editora.sepq.org.br/rpq/article/view/82

Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: A comparative analysis. *Scientometrics, 106*, 213–228. https://doi.org/10.1007/s11192-015-1765-5

Montasari, R. (2023). Internet of things and artificial intelligence in national security: Applications and issues. In *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity* (pp. 27–56). Springer International Publishing. https://doi.org/10.1007/978-3-031-21920-7_3

Moses, L. (2022). Oversight of police intelligence: A complex web, but is it enough? *SSRN Electronic Journal*, *60*(2). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4248480

Muchwa, A. S. (2021). Intelligence oversight systems in Uganda: Challenges and prospects. *Intelligence and National Security, 36*(5), 696–708. https://doi.org/10.1080/02684527.2021.1888201

Obuobi, P. P. (2018). Evaluating Ghana's intelligence oversight regime. *International Journal of Intelligence and CounterIntelligence, 31*(2), 312–341. https://doi.org/10.1080/08850607.2017.1375841

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1954824

Parsons, C. A. (2018). Law enforcement and security agency surveillance in Canada: The growth

of digitally-enabled surveillance and atrophy of accountability. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3130240

Pătrașcu, P. (2021). Emerging technologies and national security: The impact of IoT in critical infrastructures protection and defence sector. *Land Forces Academy Review*, *26*(4), 423–429. https://doi.org/10.2478/raft-2021-0055

Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know? *International Business Review, 29*(4), 101717. https://doi.org/10.1016/j.ibusrev.2020.101717

Pelizzo, R., & Stapenhurst, F. (2012). *Parliamentary oversight tools: A comparative analysis*. Routledge.

Phythian, M., Gill, P., & Marrin, S. (2008). *Intelligence theory: Key questions and debates*. Routledge.

Pires, F. M., & Andrade, A. L. (2022). Career choices: Adaptation and initial evidence of the Work Volition Scale in Brazil. *Brazilian Business Review, 19*(2), 153–170. https://doi.org/10.15728/bbr.2021.19.2.3

Polido, F. B. P. (2024). Estado, soberania digital e tecnologias emergentes: interações entre direito internacional, segurança cibernética e inteligência artificial. *Revista de Ciências do Estado*, *9*(1), 1–30. https://doi.org/10.35699/2525-8036.2024.53066

Post, C., Sarala, R., Gatrell, C., & Prescott, J. E. (2020). Advancing theory with review articles. *Journal of Management Studies, 57*(2), 351–376. https://doi.org/10.1111/joms.12549

Prince, C., Saxunová, D., & Hanson, L. (2021). Are we living in surveillance societies and is privacy an illusion? An empirical study on privacy literacy and privacy concerns. *IEEE Transactions on Engineering Management, 70*(10), 3553–3570. https://doi.org/10.1109/TEM.2021.3092702

Ribeiro, M. M. (2023). *A atividade de Inteligência de Estado brasileira está em xeque com a promulgação da Emenda Constitucional n. 115/2022?* [Dissertação de mestrado]. Universidade de Brasília.

Roberts, T., Ali, A. M., Farahat, M., Oloyede, R., & Mutung'u, G. (2021). Surveillance Law in Africa: a review of six countries. *Brighton: Institute of Development Studies*. https://doi.org/10.19088/IDS.2021.059

Shoemaker, P., Tankard Jr, J., & Lasorsa, D. (2003). *How to build social science theories*. Sage publications.

Siddaway, A. P., Wood, A. M., & Hedges, L. V. (2019). How to do a systematic review: A best practice guide for conducting and reporting narrative reviews, meta-analyses, and meta-syntheses. *Annual Review of Psychology, 70*(1), 747–770. https://doi.org/10.1146/annurev-psych-010418-102803

Snowden, E. (2019). *Eterna vigilância: Como montei e desvendei o maior sistema de espionagem do mundo*. Planeta.

Theile, C. M., & Beall, A. L. (2024). Narrative reviews of the literature: An overview. *Journal of Dental Hygiene, 98*(1), 1–10. https://jdh.adha.org/content/98/2/51

Thiry-Cherques, H. R. (2009). Saturação em pesquisa qualitativa: estimativa empírica de dimensionamento. *Revista PMKT*, 3(2), 20–27.

União Europeia. (2023). *Relatório A9-0189/2023*. Parlamento Europeu. https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_PT.html

Van Brakel, R. (2021). How to watch the watchers? Democratic oversight of algorithmic police surveillance in Belgium. *Surveillance & Society, 19*(2), 228–240. https://doi.org/10.24908/ss.v19i2.14325

Veletsianos, G., & Shepherson, P. (2016). A systematic analysis and synthesis of the empirical MOOC literature published in 2013-2015. *International Review of Research in Open and Distributed Learning, 17*(2), 198–221. https://doi.org/10.19173/irrodl.v17i2.2448

Vieth, K., & Wetzling, T. (2020). Data-driven intelligence oversight: Recommendations for a system update. *SSRN Electronic Journal*. https://dx.doi.org/10.2139/ssrn.3505906

Walsh, P. F. (2022). Australian intelligence oversight and accountability: Efficacy and contemporary challenges. *Intelligence and National Security, 37*(7), 968–984. https://doi.org/10.1080/02684527.2022.2095602

Wegge, N. (2017). Intelligence Oversight and the Security of the State. *International Journal of Intelligence and CounterIntelligence*, *30*(4), 687–700. https://doi.org/10.1080/08850607.2017.1337445

Weinstein, J. M., Moore, R. J., & Silverman, N. P. (2017). Balancing privacy and public safety in the post-Snowden era. In D. Gray & R. Henderson (Eds.). *The Cambridge handbook of surveillance law* (pp. 227–247). Cambridge University Press. https://doi.org/10.1017/9781316481127

Wills, A., & Vermeulen, M. (2011). *Parliamentary oversight of security and intelligence agencies in the EU*. European Parliament.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems, 22*(1), 45–55. https://doi.org/10.1057/ejis.2011.51

Xu, X. (2021). To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance. *American Journal of Political Science*, *65*(2), 309–325. https://doi.org/10.1111/ajps.12514

Young, M., Katell, M., & Krafft, P. M. (2019). Municipal surveillance regulation and algorithmic accountability. *Big Data & Society, 6*(2), 205395171986849. https://doi.org/10.1177/2053951719868492

Zairi, M. (2010). *Benchmarking for best practice*. Routledge.

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. In *New labor forum, 28*(1), 10–29. Sage Publications. https://doi.org/10.1177/1095796018819461

Zuboff, S. (2020). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.

Zuboff, S. (2022). Surveillance capitalism or democracy? The death match of institutional orders and the politics of knowledge in our information civilization. *Organization Theory, 3*(3), 26317877221129290. https://doi.org/10.1177/26317877221129290

Conrado Klöckner

Master in Public Administration from Brazilian School of Public and Business Administration at Getulio Vargas Foundation (FGV EBAPE); Legislative Director at the Rio Grande do Sul State Assembly. E-mail: conradoklockner@gmail.com

Luiz Antonio Joia

Full Professor at the Brazilian School of Public and Business Administration at Getulio Vargas Foundation (FGV EBAPE). E-mail: luiz.joia@fgv.br

AUTHORS' CONTRIBUTIONS

Conrado Klöckner: Conceptualization (Lead); Data Curation (Lead); Formal Analysis (Lead); Funding Acquisition (Lead); Investigation (Lead); Methodology (Lead); Project Administration (Equal); Resources (Lead); Software (Lead); Supervision (Supporting); Validation (Equal); Visualization (Equal); Writing – Original Draft (Lead); Writing – Review & Editing (Supporting).

Luiz Antonio Joia: Conceptualization (Supporting); Data Curation (Supporting); Formal Analysis (Supporting); Funding Acquisition (Supporting); Investigation (Supporting); Methodology (Supporting); Project Administration (Equal); Resources (Supporting); Software (Supporting); Supervision (Lead); Validation (Equal); Visualization (Equal); Writing – Original Draft (Supporting); Writing – Review & Editing (Lead).

DATA AVAILABILITY

All datasets supporting the findings of this study have been made available through the FGV Library System and can be accessed at https://repositorio.fgv.br/items/af86cd33-d297-4465-8d12-4a27634e4899.

FUNDING

This research was funded by the Brazilian National Council for Scientific and Technological Development (CNPq), grant number 304290/2021-1 (L.A.J.), and by the Brazilian School of Public and Business Administration at the Getulio Vargas Foundation (FGV EBAPE), grant number PROPESQUISA 00505100300360 (L.A.J.).